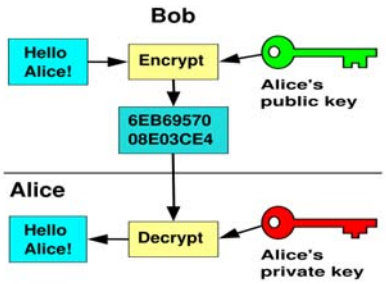
91.113 Exploring the Internet, Fall 2011

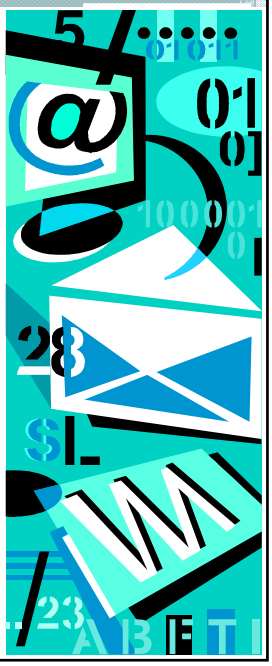
Lecture 20. Encryption on the Internet



Instructor: Jie Yang
Department of Computer Science
University of Massachusetts Lowell

Learning Objectives

- Understand how private-key and public key encryption work.
- Learn how digital signatures protect document integrity.
- Understand why key authentication is needed to protect people from counterfeit keys.
- Find out how digital certificates and certificate authorities solve the problem of key authentication.
- Understand the difference between strong and weak encryption.



Taking Charge

- **Cryptography** is the study of secret codes associated with classified information and intelligence gathering.
- The National Security Agency (NSA) is responsible for developing and applying secure communication technologies in the service of national security.
- Cryptography used to be only of interest to the military.
- As digital communication is more widespread, it is of interest to more of us.

- Cryptography is of interest to:
  - Client/server software developers
  - Anyone interested in digital commerce
  - All Internet users who want to keep their communications private
- Without safeguards, our sensitive information is at risk.
- Cryptography offers protection.

- We don’t all work for the military or a large organization, but we want privacy safeguards too.
- This chapter will introduce the basic concepts for encryption.

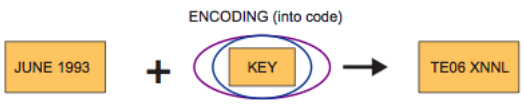
Private-Key Encryption

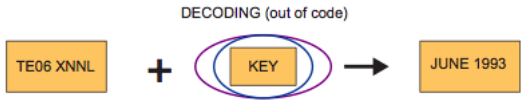
- **Encoding** and **decoding** information is key to encryption.
- Plain text => Encryption => Ciphertext
- A key for a simple substitution code is just a map that tells you how to substitute one character for another.
- When you receive a coded message, you trade each character for a new one according to the instructions on the key.

- **Encoding** is the process of creating the coded message.
- **Decoding** is the process of unscrambling the coded message.
- To encode a message, you *must* use the same key when decoding (though you have to reverse the key).
- Private-key encryption is the use of the same key for encoding and decoding messages.

Symmetric key cryptography:

A→H	F→7	K→A	P→5	U→E	Z→?	5→D	/→W
B→C	G→0	L→.	Q→F	V→S	1→X	6→R	.→Q
C→4	H→B	M→V	R→1	W→Z	2→P	7→K	!→G
D→I	I→M	N→0	S→!	X→J	3→L	8→Y	?→U
E→6	J→T	0→3	T→9	Y→2	4→8	9→N	



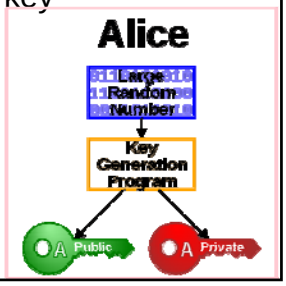


- If you have the key for the code, it is easy to decode messages.
- If you don't have the key, then
  - You can try and break the code
  - Or try and figure out the key if you have several messages
- To figure out such a key,
  - Try and find commonly used letters
  - The letter "e" is the most common
  - Try and decipher common words (e.g."the")

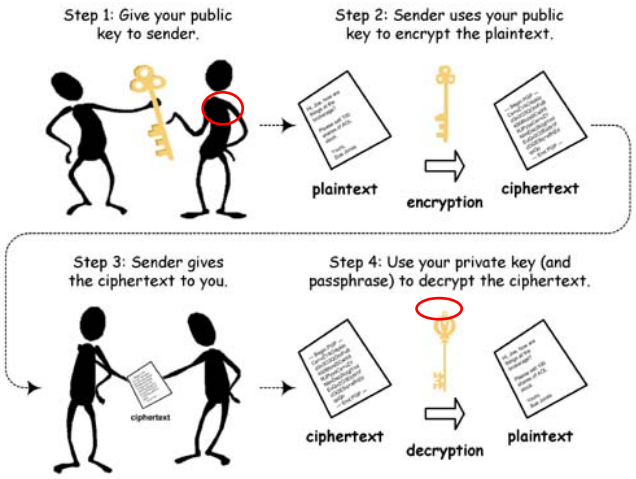
- Private-key encryption is risky since many people share the same key.
- Each time the key is passed from person to person, it may be intercepted.
- If the information that you are sharing is not critical, then you can evaluate the risk.

Public-Key Encryption

- If your information is more important, then you may choose to use public-key encryption.
- **Public-key** encryption uses 2 keys, which is more secure than private-key encryption.
- If one of the keys is lost, the other key is useless by itself.
- These 2 keys are generated as a special key pair that works together.



- The 2 keys consist of:
  - A public key that can be freely distributed to anyone and everyone
  - A private key is held by only the owner of the key pair
- Although both keys are needed, having the public key available does not make it possible to decipher the private key.

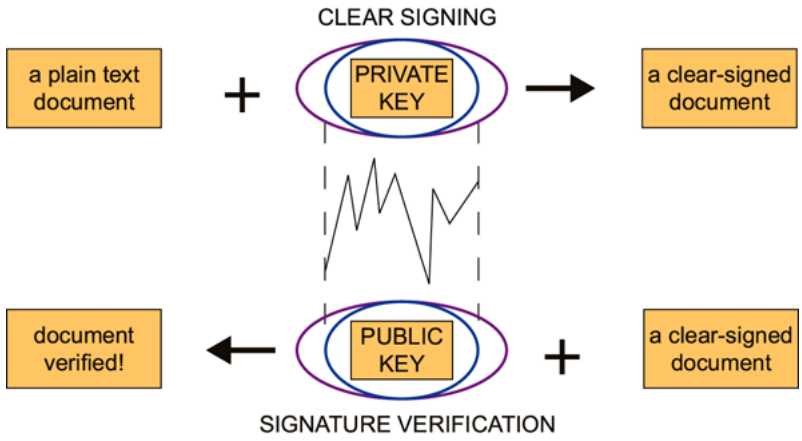


- If you want to receive encrypted messages
  - You create a pair of keys
  - You can give copies of the public key to anyone (but you keep your private key)
  - The public keys are used to encode messages
  - Your private key is used to decode messages
- Only your private key can decode messages encoded by your public key.

Digital Signatures

- Like signatures on paper, when a document is signed you know who wrote it or approved its contents.
- Written signatures can be forged
- Digital signatures need to be resistant to forgery.
- Public-key encryption is used to make digital signatures forgery-resistant.
- Digital signatures are important for e-commerce and other sensitive communication.

- A clear signature is a digital signature that is attached to a plain-text file.
- A clear-signed document is a document signed with a clear signature.
- The process of generating and verifying a digital signature is similar to the process of encrypting and decrypting a file.



- Digital signatures change from document to document.
- A digital signature contains information
  - about the person behind the signature
  - about the document being signed
- So one digital signature cannot be copied from one document to another

Key Management

- Public-key encryption makes it easier to keep a private key private.
- If you store a private key, you must be able to protect that key.
- Protecting your private-key with a passphrase helps secure your key.
- Whenever you create a key pair, you enter a passphrase.
- Whenever you need to use your private-key to decode a message, you must enter your passphrase.

Counterfeit Keys

- A security hole remains where a hacker can generate a key pair under your name and intercept messages.
- This is called the Man-in-the-Middle attack.

Man in the middle attack

Trudy poses as Alice (to Bob) and as Bob (to Alice)

Difficult to detect:

- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation)
- problem is that Trudy receives all messages as well!

- Public-keys are subject to scrutiny.
- You need to know who owns the keys that you use to encrypt information.
- You need to trust that the information you receive is from the sender of the message.
- A public-key is said to be a trusted key when you are certain that the key is not counterfeit.
- The process of identifying a person as the legitimate owner of a public key is called **key authentication.**

Key Certification

- A system of key certification is needed to help people decide how much risk is associated with any given pubic-key.
- Key certification is the process through which someone can vouch for the legitimacy of a pubic key.
- When a key is certified by a trusted friend, that person can add his or her digital signature to the public key being certified.
- Then if the key is sent to you, you can verify the digital signature with confidence

- The model for key certification based on friends (and their friends) is called the “Web of Trust”
- Public keys are passed among friends, accumulating certification as they go.
- This model works well in small worlds.
- When communities become large, this model is not viable.

- A digital fingerprint for a key pair is a unique sequence of integers associated with that key pair.
- Digital fingerprints are generated when a key pair is created, based on random conditions
- The fingerprint cannot be tampered with.
- Fingerprint verification is an alternative to the Web of Trust, but it's still not good for large communities (e.g. for e-commerce)

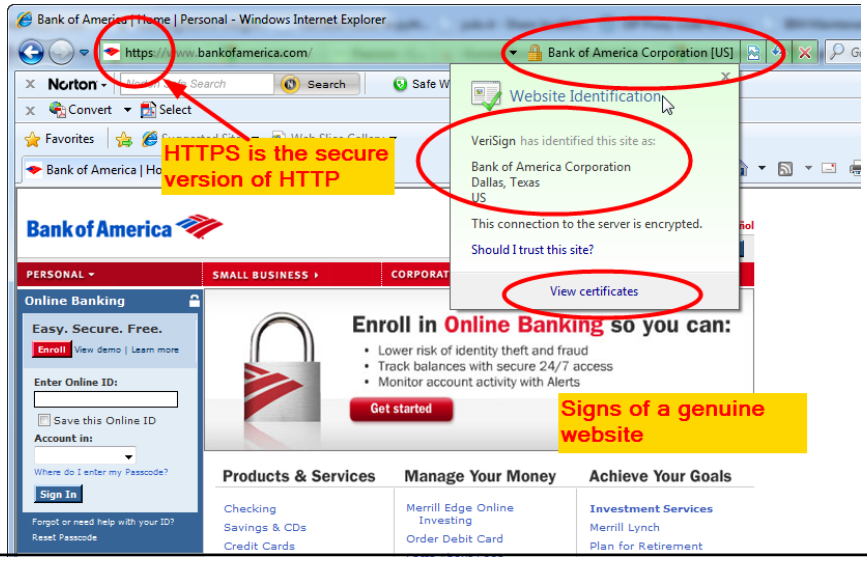
Digital Certificates

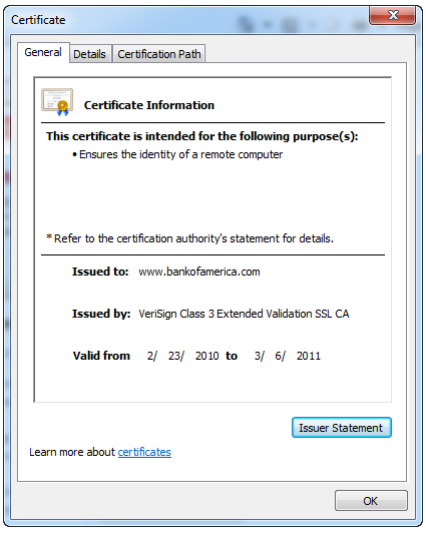
- The problem of key authentication had to be solved before public-key encryption could be used for e-commerce.
- Without a system for certifying valid public keys, counterfeit pages could masquerade as legitimate e-stores.
- A digital certificate is a digital signature attached to a public key.
- The purpose of the certificate is to reassure users that the public-key is the authentic key.

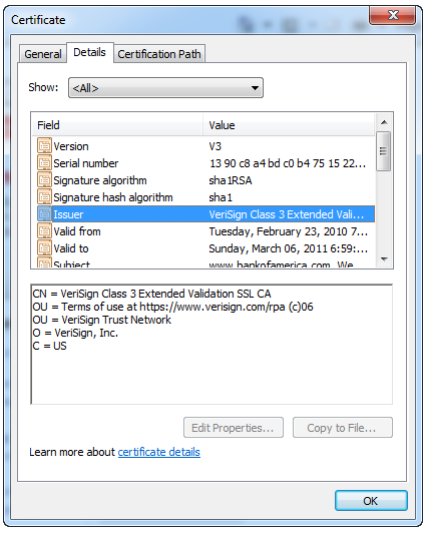
- In the Certificate Authority (CA) model of key authentication, there are only a few trusted institutions that can generate digital certificates.
- Any key generated by a trusted CA can be immediately trusted without question.
- All the user has to do is decide which CAs can be trusted.

- If you placed a credit card order online, your browser probably checked server certificates for you and you didn't know it.
- Your browser has a list of trusted Cas built into it.
- Your browser will then accept any public-key certified by a recognized CA.
- You can check the settings in your browser.

Digital Certificates







Strong and Weak Encryption

- When people worry about whether they can trust encryption, they generally are concerned about how hard it is to crack.
- The amount of time needed to crack a code is important.
- 40-bit keys can be broken by run-of-the-mill personal computers in minutes.
- Any key that can stand up to thousands of years of computing time on the fastest computers is safe enough.

- Strong encryption refers to encryption methods that are safe in this sense.
- A code that can be broken in a practical time frame is called weak encryption.
- Strong encryption steadily becomes weaker over time.
- Taking Moore's law into consideration
  - 64-bit encryption will be weak by 2011
  - 128-bit encryption will be weak by 2107